UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

UNITED STATES OF AMERICA,	)	
	)	
v.	)	No. 3:08-CR-142
	)	Judges Phillips/Shirley
DAVID C. KERNELL,	)	
a/k/a "rubico,"	)	
a/k/a "rubico10,"	)	
	)	
Defendant.	)	

OPPOSITION TO DEFENDANT'S SECOND MOTION TO SUPPRESS AND MOTION FOR EVIDENTIARY HEARING

The United States of America, by and through James R. Dedrick, United States Attorney for the Eastern District of Tennessee, respectfully submits this response to Defendant's Second Motion to Suppress and motion for evidentiary hearing. (Doc. 69).

Defendant's new suppression motion can be denied for the same reasons as the first one: The September search warrant, amply supported by probable cause, indisputably authorized the search of Defendant's apartment, indisputably authorized the seizure of Defendant's Acer laptop, (Doc. 69 at 23), and indisputably noted the necessity of an "examin[ation of] all the stored data to determine which particular files are evidence, contraband, fruits, or instrumentalities of criminal activity," (Ex. A ¶ 32a); (*see also* Doc. 20 at 6) (defense acknowledging search warrant permitted seizure of "some of his computer files")), and allowed for the seizure of records particularly described. (Ex. A, Att. B). Consequently, the probable cause and authority under the September search warrant resolves both motions to suppress. The February search warrant,

while not required, provided a second review by a detached, neutral magistrate judge, based on new charges and the ongoing investigation, and merely gave Defendant further protection.

Defendant's argument that the agents executed the warrant improperly is entirely unfounded. It is not surprising that Defendant, despite multiple opportunities to do so, is unable to articulate any basis in which the search warrant was executed improperly. Defendant simply repeats his attack on the examiner's decision to employ a particular search technique, even though that technique was approved in advance by the reviewing magistrate judge and has been endorsed by this Court, by the Sixth Circuit, and by every other circuit court to consider the issue. After entirely ignoring *his threshold burden* to show contested issues of fact going to the validity of the search, Defendant asks for a hearing anyway, frankly acknowledging its only purpose would be to allow Defendant to learn facts for the first time — a plainly illegitimate ground for an evidentiary hearing. (Doc. 69 at 27). As noted at the last hearing, on such a bare record, if the defense motion were granted, it could be used to justify similar fishing expeditions in other search warrant challenges. For these reasons, and others given below, Defendant's two motions to suppress and his new motion for a discovery "evidentiary" hearing should be denied.

I. THE FIRST SEARCH WARRANT LAWFULLY AUTHORIZED THE SEARCH OF THE APARTMENT, THE SEIZURE OF THE COMPUTER, AND THE SUBSEQUENT SEARCH THROUGH THAT COMPUTER.

A valid warrant, supported by probable cause, authorized both the seizure of Defendant's computer and the subsequent search of Defendant's computer for things particularly described on the warrant. This warrant, and its reasonable execution, requires rejection of Defendant's motions to suppress. As noted at the last hearing, the Court can do so based on the probable cause and authority under the September search warrant alone.

On September 20, 2008, a few days after the September 16, 2008 attack on Governor Palin's account, FBI Special Agent Andrew Fisher obtained a search warrant to search Defendant's apartment for evidence of the attack. The affidavit in support of that warrant describes how agents connected Defendant's online postings to an e-mail account, (Ex. A ¶ 15), connected that e-mail account to a particular Internet Protocol ("IP") address used to access it, (Ex. A ¶ 18), and connected that IP address to the apartment building and apartment where Defendant resides, (Ex. A ¶ 18). It also described how Defendant's roommates told agents that Defendant was discussing breaking into Sarah Palin's e-mail account, (Ex. A ¶¶ 21-28), including one occasion where "Kernell advised [his roommate] that he had succeeded in breaking into Palin's e-mail account," (Ex. A ¶ 24). Based on this information, the affidavit and search warrant requested seizure and examination of an "Acer brand laptop computer." (Ex. A, Att. B ¶ 2).

The first warrant included a particularized list of things to be seized, including records "related to or referring to the e-mail addresses of or the name Sarah Palin," (*Id*. ¶ 4), and for "[d]ocuments and computer files in any form" that are "related or… associated with" a list of e-mail addresses and online monikers that the affidavit had all linked with either a victim or Defendant, as well as with "hacking activities." (*Id*. ¶ 1). The affidavit in support of the warrant explained how it is often necessary to seize an entire computer and later analyze it offsite, a process that in some cases requires "examin[ing] all the stored data to determine which particular files are evidence, contraband, fruits, or instrumentalities of criminal activity," (Ex. A ¶ 32a).

Against this background, it is notable what Defendant does not challenge. Defendant does not dispute that the facts in the affidavit establish probable cause to search his apartment. In fact, Defendant "agrees that the first warrant authorized the seizure of the computer." (Doc.

69 at 23). Defendant has previously also agreed that the warrant authorized the seizure of "some of his computer files." (Doc. 20 at 6). In discovery, Defendant received a copy of his seized hard drive and a forensics report which describes the files obtained during the examination. Defendant does not argue that any of those files falls outside the list of things to be seized in the first warrant.

Instead, Defendant's sole and narrow argument for suppression is that "the manner of the execution of the search warrant was unconstitutional." (Doc. 69 at 8). Defendant makes two sub-arguments in support: (1) Defendant repeats the argument that searching through the hard drive for the things called for by the warrant was improper, and (2) Defendant argues the forensic exam had to be completed in ten days. As discussed below, Defendant supports neither of these arguments with facts or law, and an avalanche of cases has rejected each. The government respectfully urges this Court to do the same.

A. The warrant authorized the search of the entire hard drive, and this authorization was proper under the Fourth Amendment.

Defendant repeats the argument that searching through the hard drive for the things called for by the warrant (and, in the process, viewing things not called for by the warrant) was improper. Defendant forces this argument to serve triple duty by arguing, alternately, that the warrant lacked probable cause to look at irrelevant files, (Doc. 69 at 23), that the irrelevant files were not particularly described, (Doc. 69 at 13), and that any warrant that authorized such a search was unconstitutionally general (Doc. 69 at 14).

The United States rebutted this argument, in all its forms, in its opposition to Defendant's last motion to suppress: both Judge Greer of this Court and the Sixth Circuit have agreed that it is permissible to seize an entire computer and then search it off-site for those things authorized to be seized. *See* Doc. 22 at 3-4; *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001); *United States v.*

Tillotson, No. 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008). Defendant cites no courts that rejected this technique.

In fact, many other courts have accepted it. *See United States v. Giberson,* 527 F.3d 882, 889-90 (9th Cir. 2008) (permitting search of every image file on a computer); *United States v. Khanani,* 502 F.3d 1281, 1290 (11th Cir. 2007) (endorsing a search in which "a computer examiner eliminated files that were unlikely to contain material within the warrants' scope"); *United States v. Brooks,* 427 F.3d 1246, 1251-53 (10th Cir. 2005) (approving "a warrant that authorized officers to search through computer files for particular items specifically related to child pornography"); *United States v. Jack,* 2009 WL 453051, *4 (E.D. Cal. 2009) ("it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence"); *United States v. Fumo,* 565 F.Supp.2d 638, 649 (E.D. Pa. 2008) ("[B]ecause of the nature of computer files, the government may legally open and briefly examine each file when searching a computer pursuant to a valid warrant"); *Manno v. Christie,* 2008 WL 4058016 (D. N.J. 2008) (finding it "reasonable for [agent] to briefly review each electronic document to determine if it is among the materials authorized by the warrant, just as he could if the search was only of paper files"); *United States v. Potts,* 2008 WL 2051090 *11 (D. Kan. 2008) (finding a warrant did not authorize an overbroad search when it allowed the investigator "to search the computer by... opening or cursorily reviewing the first few 'pages' of such files in order to determine the precise content" (internal quotation marks removed)).

What's more, the reviewing magistrate judge approved that procedure in this case. The warrant affidavit said that "it is often necessary that some computer equipment… be seized and subsequently processed by a qualified computer specialist in a laboratory setting." (Ex. A ¶ 32).

It advised that "the [computers] themselves may be instrumentalities, fruits, or evidence of crime" as well as "used to collect and store information about crimes (in the form of electronic data)." (Ex. A ¶ 30). It plainly informed the reviewing magistrate judge that in some cases "[s]earching authorities are required to ***examine all the stored data*** to determine which particular files are evidence, contraband, fruits, or instrumentalities of criminal activity." (Ex. A ¶ 32a) (emphasis added). Here, it is undisputed that the seized Acer laptop was not only an instrumentality of the criminal activity but also contained evidence of the offense. In fact, this has been confirmed in the forensic report provided to the defense.

While Defendant argues that the second warrant contradicted the first, (Doc. 69 at 12-18), in fact the second search warrant said much the same thing: after saying that a "targeted search[]" might not "yield the evidence described in the warrant," it advised that agents might be required to "conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or perus[ing] ***every file*** briefly to determine whether it falls within the scope of the warrant," (emphasis added) and concluded that agents would "use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A." (Ex. B ¶ 19).

This affidavit language requires the rejection of any argument that agents acted with "disregard" for the warrant. (Doc. 69 at 8, 18). To the contrary, they did exactly what the warrant described. Including this language in the affidavit "documented the informed endorsement of the neutral magistrate" to the search technique that was used, *United States v. Hill*, 459 F.3d 966, 977 (9th Cir. 2006), thereby providing the Defendant with additional procedural protection.

In sum, the first search warrant was supported by ample probable cause for the seizure and examination of Defendant's Acer laptop. The first search warrant affidavit noted the necessity of "examin[ing of] all the stored data to determine which particular files are evidence, contraband, fruits, or instrumentalities of criminal activity." (Ex. A ¶ 32a). The execution of the search warrant confirmed that the laptop was an instrumentality and contained evidence of the offense. The motions to suppress can be resolved on the first search warrant alone. The second search warrant, providing further judicial review based on new charges and the ongoing investigation, merely gave further protection to Defendant. The motions can readily be denied.

B. The forensic examination of Defendant's hard drive occurred within a constitutionally reasonable time.

Defendant argues that the forensic exam was unreasonable because it look longer than ten days. (Doc. 69 at 18-22). Defendant does not cite a single case that supports suppression on this ground. Not surprisingly, courts have roundly rejected it.

When law enforcement seizes a hard drive, "neither Rule 41 nor the Fourth Amendment impose any time limitation on the government's forensic examination of the evidence seized." *United States v. Triumph Capital Group, Inc.,* 211 F.R.D. 31, 66 (D. Conn. 2002). So long as investigators physically enter premises and seize the computer during the ten-day period, the subsequent forensic examination can occur after the ten-day period. *See United States v. Mutschelknaus,* 564 F.Supp.2d 1072, 1077 (D. N.D. 2008) (forensic exam 52 days after the 10-day deadline); *Matter of the Search of the Scranton Housing Authority,* 436 F.Supp.2d 714, 727 (M.D. Pa. 2006), *vacated on other grounds,* 487 F.Supp.2d 530 (M.D. Pa. 2007) (forensic exam that continues "up to this day" valid on computer seized more than a year earlier); *United States v. Hernandez,* 183 F. Supp.2d 468, 480 (D.P.R. 2002) (forensic exam 36 days after the 10-day deadline); *United States v. Habershaw,* 2002 WL 33003434, at *8 (D. Mass. 2002) (forensic

exam 4 days after the 10-day deadline); *Triumph Capital*, 211 F.R.D. at 66. Each of those cases involved the same facts: a federal search warrant was issued under Rule 41, commanding a search within 10 days; law enforcement seized the computer within those 10 days; and law enforcement then conducted forensic examination after the 10 days. In each case, the court was satisfied that the warrant was complied with because the evidence came into law enforcement's possession within the required 10 days, even though the analysis of that evidence was not complete within that time. Additionally, in a case dealing with a state search warrant, the First Circuit held in *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005), that "[t]he Fourth Amendment itself contains no requirements about when the search or seizure is to occur or the duration," other than "reasonableness." *Id.* at 469 (quotation marks omitted)*; see also Commonwealth v. Ellis*, 1999 WL 815818, *9 (Mass. Super. 1999) ("The ongoing search of the computer's memory need not have been accomplished within the seven-day period required for return of the warrant").

These courts all understood the reason for the 10-day rule. "The policy behind the ten-day time limitation in Rule 41 is to prevent the execution of a stale warrant." *Syphers*, 426 F.3d at 469. However, when hard drives are seized, the evidence that they contain is "frozen in time," obviating the staleness concerns present with other warrants. *Scranton Housing Authority*, 436 F.Supp.2d at 728. "As long as the search time is reasonable under the circumstances, the continued off-site search will not violate the Fourth Amendment." *Id.*

Indeed, by now this rule is so universal and uncontroversial that it will soon be codified into Rule 41. In an amendment scheduled to take effect on December 1, 2009 (barring contrary Congressional action), Rule 41 will read, in part:

> *Warrant Seeking Electronically Stored Information.* A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic

> storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. ***The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.***

Amendments to the Federal Rules of Criminal Procedure at 21, available at http://is.gd/1RD8a (emphasis added).

Defendant appears to argue that forensic examination must be completed with what amounts to lightning speed. Countless courts have recognized, however, that "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution." *Triumph Capital,* 211 F.R.D. at 66. In this case, Defendant points to no way in which he has been prejudiced by the forensic examination's length. The affidavit in support of the first warrant explicitly advised that the forensic examination could "take weeks or months, depending on the volume of data stored." (Ex. A ¶ 32a). Including that language in the affidavit "documented the informed endorsement of the neutral magistrate." *United States v. Hill,* 459 F.3d 966, 977 (9th Cir. 2006).

Defendant invites this Court to be the first in the nation to place a ten-day time limit on forensic examination. In support, Defendant emphasizes a single case, *United States v. Mitchell,* 565 F.3d 1347 (11th Cir. 2009). Defendant summarizes *Mitchell* for three and a half pages of his brief, (Doc. 69 at 19-22), but its inapplicability to his argument can be summarized in a single sentence: *Mitchell* involved a ***warrantless*** seizure of a hard drive, does not even mention the 10-day rule, and does not discuss the permissible time period for a forensic examination at all.

In a variation on this argument, Defendant argues that the "delay" in obtaining the second warrant was too long under *Mitchell*. But *Mitchell* turned on the length of time that the

defendant in that case was deprived of the "possessory interest" of his hard drive without a warrant. *Mitchell,* 565 F.3d at 1351. In this case, as Defendant concedes, the first warrant authorized the seizure of his hard drive. (Doc. 69 at 23) ("Mr. Kernell agrees that the first warrant authorized the seizure of the computer"). Therefore, Defendant has no parallel argument that his possessory interests were ever intruded upon without a warrant.

C. The first warrant was valid, and nothing in the second warrant's supporting affidavit contradicted the first warrant's affidavit.

Defendant argues that the act of obtaining the second warrant was, by itself, an "admission" that the first was invalid. (Doc. 69 at 11, 2). It was not. Defendant cites no case holding that the act of obtaining a second warrant constitutes an "admission" that the first was invalid, and cites no case holding that a second warrant in any way retroactively diminishes the authority of the first warrant. Instead, Defendant discourses for pages on the irrelevant subject of judicial estoppel, citing no cases that found estoppel arising from a probable cause affidavit. (Doc. 69 at 14-18).

If anything, a second warrant *affirms* the constitutionality of a search. A warrant application "interpose[s] a neutral and detached magistrate between the citizen and the officer." *United States v. Karo,* 468 U.S. 705, 717 (1984) (quotation marks removed). Doing this twice, rather than once, can only augment a defendant's protection under the Constitution; it cannot possibly support suppression. Defendant's "admission" argument, then, lacks not only law, but logic. It is akin to arguing that a man who puts on suspenders after he has already put on a belt has made an "admission" that his pants are lying around his ankles.

The United States obtained a second warrant not because the first was invalid, but based on "evidence obtained during the continuing investigation," as well as a recent "superseding Indictment in this case" and other identified charges. (Ex. B ¶ 3). It was not a requirement,

given the ample probable cause and express authority in the first search warrant, but merely a matter of prudence. The practice of obtaining an additional warrant in such a circumstance is a sensible precaution, because some courts have warned against "expanding the scope of the search without obtaining a second warrant." *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir. 2000). Though unnecessary — especially here, where Defendant ultimately did not argue that any file obtained by the examiner fell outside the warrant — the second consultation with a detached and neutral magistrate judge about the appropriate scope of the search furthered the goal of protecting Defendant's rights. Defendant cannot claim, and does not argue, he was prejudiced by the second search warrant.

Defendant mischaracterizes the second warrant's supporting affidavit as "admit[ing]" certain things (Doc. 69 at 2, 4 n.6, 11, 12-14). A review of the second search warrant affidavit "admits" no such things. (Ex. B). The second search warrant affidavit provided an update on the new charges and other developments in the ongoing investigation. At no point does the affidavit ever state that the affiant believed he lacked judicial authority for a forensic examination of the computer (Doc. 69 at 2), that limiting protocols could be used in this case (Doc. 69 at 4 n.6, 11), or that he lacked authority for an "extensive" search (Doc. 69 at 12-14). Defendant fails to cite any words in the affidavit saying any such thing. They are not there.

Defendant focuses on a single sentence in that affidavit: "In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence." This sentence simply advised of the possibility, however remote, that "in some cases" searches are easy. For example, although, as a general rule, "[f]iles on computers containing child pornography likely would not be identified as 'My Child Porn,'" *United States*

v. Tillotson, 2008 WL 5140773, *4 (E.D. Tenn. 2008), in a case where such a folder ***does*** exist on a hard drive, a targeted search of it might be all that is necessary to find child pornography. This is not, as Defendant argues, a statement that ***all*** searches are easy, or that the search in ***this case*** is that easy.

Indeed, the full context of the paragraph makes it clear that the "targeted search" is an option that can be used only when circumstances permit. Defendant quotes the surrounding sentences only once, and then only in a block, (Doc. 69 at 7), but they are crucial.[1] The affidavit describes a "range of data analysis techniques" that can be used based on what is "possible" in the particular "case" at hand. (Ex. B ¶ 19). The "targeted search" Defendant emphasizes was one possible end of that "range." However, the affidavit was clear that such a targeted search "may not yield the evidence described in the warrant." *Id.* Thus, at the other end of the range was "more extensive searches," which included "perus[ing] ***every file*** briefly to determine whether it falls within the scope of the warrant"—the technique used here. *Id.* (emphasis added). In explaining how agents determine which techniques along that "range" are required in a particular circumstance, the affidavit noted as an example that "[c]riminals can… take other

[1] The relevant paragraph, number 19, reads in full:

> Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

steps designed to frustrate law enforcement searches for information," such as "delet[ing] files." As the affidavit noted, the Grand Jury found probable cause to believe that Defendant had done just that. (Ex. B at ¶ 9h).

Consequently, it is simply wrong and unfounded for Defendant to claim that the affidavit demonstrates "the government was really making a choice to reject the technological or judicial mechanisms that are available to limit a computer search." (Doc. 69 at 12). If anyone made that "choice," it was Defendant: he is the one who organized (or disorganized) his hard drive. The affidavit makes clear that the circumstances of each case control. While a defendant could conceivably cite specific facts that could question whether agents chose the correct technique along that "range," Defendant has failed to do so here: Defendant's brief is bereft of any explanation of how his hard drive could have been searched in such a "targeted" fashion. Nor is it acceptable for Defendant to claim he could not brief this issue because he does not know what the agents did. (Doc. 69 at 8). On this issue, the relevant facts are not what the examiner did, but whether a reasonable examiner would have determined from the organization of Defendant's hard drive that a targeted search was appropriate. Defendant's failure, after full discovery (which included a complete copy of his hard drive), to point to anything on his hard drive that would have invited a targeted search is fatal to his argument. Again, the failure to make this argument underscores the Defendant's inability to satisfy his threshold burden to permit his requested fishing expedition.

In short, the first search warrant was supported by probable cause, stated with particularity the things to be searched and seized, and was approved by a detached and neutral magistrate judge. To the extent Defendant challenges its execution, Defendant challenges only the forensic examination, and even then never challenges the examiner's decision to seize any

specific file. Instead, Defendant effectively challenges the constitutionality of computer forensics in general. Defendant does so while citing no case endorsing his theory, though almost a decade of settled precedent at the district and circuit court levels reject it. Consequently, Defendant's motion for suppression must be denied.

II. DEFENDANT HAS NOT MADE THE REQUIRED SHOWING FOR AN EVIDENTIARY HEARING ON HIS MOTION TO SUPPRESS.

A. Neither of Defendant's two challenges to the forensic process involve contested issues of fact that require a hearing.

"An evidentiary hearing is required only if the motion is sufficiently definite, specific, detailed, and non-conjectural to enable the court to conclude that ***contested issues of fact*** going to the validity of the search are in question." *United States v. Abboud*, 438 F.3d 554, 577 (6th Cir. 2006) (quotation marks omitted; emphasis original). While Defendant writes that "the manner in which a forensic search of a computer is conducted and the extent to which it exposes lawful conduct is a relevant inquiry for an evidentiary hearing," (Doc. 69 at 9), Defendant offers only two arguments about why the forensic examination here was improper, neither resting on contested issues of fact.

First, Defendant repeats the argument that searching through the hard drive for the things called for by the warrant (and in the process viewing things not called for by the warrant) was improper. (Doc. 69 at 13, 14, 23). But, as noted at the last hearing, whether there was an examination of all files on defendant's computer is not disputed. Not only was the examination of "all the stored data to determine which particular files are evidence, contraband, fruits, or instrumentalities of criminal activity" noted in the first search warrant affidavit, (Ex. A ¶ 32a), this issue is purely legal; it cannot be resolved with an evidentiary hearing. *See Abboud*, 438 F.3d at 577 ("Defendant did not agree with the magistrate's legal decision based on the facts.

This type of disagreement is not resolved through an evidentiary hearing."). This issue is fully briefed for the Court. (*See supra* Part I.A).

Second, Defendant argues that the forensic examination had to be completed within ten days after the warrant was issued. It is undisputed that the forensic examination was not completed during this period of time. Again, this issue is purely legal and covered by prior case law. This issue is also fully briefed for the Court. (*See supra* Part I.B).

Thus, to the extent that Defendant challenges the manner of execution of the warrant at all, his challenge rests on no contested issues of fact and thus an evidentiary hearing would be improper and unnecessary. Defendant has acknowledged at the prior hearing and second motion that he has no contested facts but merely hopes that an evidentiary hearing may provide some. Based on the record before the Court, Defendant should not be allowed to fish for facts in support of his unfounded arguments.

B. Defendant bears the burden on a motion to suppress, and thus is not entitled to an evidentiary suppression hearing merely as a tool for discovery.

Failing to point to any facts that would support his argument that the forensic examiner acted unreasonably, Defendant asks for a hearing to fish for facts that might support his argument. Defendant's brief frankly states that "Mr. Kernell cannot state the facts with precision without an evidentiary hearing," (Doc. 69 at 3 n.3), and even appears to argue for a rule that "[t]he reasonableness of a search… requires an evidentiary hearing" *in every case,* (Doc. 69 at 14).

A dearth of facts in support of a motion to suppress is not grounds for a hearing; it is grounds for denying the motion. Defendant has the burden: "the law is clear in this circuit that 'the burden of production and persuasion rests on the person seeking to suppress evidence.' " *United States v. Giacalone,* 853 F.2d 470, 482 (6th Cir. 1988), *quoting United States v. Smith,*

783 F.2d 648, 650 (6th Cir.1986). That burden is met only with a "motion [that] is sufficiently definite, specific, detailed, and non-conjectural to enable the court to conclude that ***contested issues of fact*** going to the validity of the search are in question," *United States v. Abboud*, 438 F.3d 554, 577 (6th Cir. 2006) (quotation marks omitted; emphasis original). Defendant's frank statement that he "cannot state the facts with precision without an evidentiary hearing" accompanies a brief in which he states no facts, at all, that support his arguments for suppression. (Doc. 69 at 3 n.3). A bare desire for a hearing is not enough; "the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Franks v. Delaware*, 438 U.S. 154, 171 (1978). The Supreme Court in *Franks* warned that evidentiary suppression hearings could be "misused by defendants as a convenient source of discovery"; Defendant appears to be asking for just such a misuse. *Franks*, 438 U.S. at 167.

It is true that "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979). The mechanism for such a review, however, is a motion to suppress supported by fact and law, and the Defendant bears the burden with such a motion. It is up to Defendant to raise some sort of legal argument as to *why* the manner in which the warrant was executed was unreasonable.

The Court granted Defendant the opportunity to file this second motion in part so that Defendant could take advantage of that procedure. This required Defendant to buttress his arguments with facts gleaned from discovery about the forensic examination of his hard drive. Yet, Defendant's motion does not point to a single piece of discovery that supports his argument. This is telling. Through discovery, defendant now has access to a sector-by-sector copy of his hard drive. If there were any facts to support Defendant's argument that a "targeted" search of that hard drive was appropriate, (Doc. 69 at 11-12), it is Defendant's burden at least to explain

why by pointing to specific files, folders, or otherwise identifying a less intrusive search strategy that would have been apparent to a reasonable examiner and would have located the same things called for by the warrant. Defendant also now has the forensic examiner's report, which identifies the files and things the examiner located that might be introduced at trial. If there were any facts to support Defendant's argument that "the manner in which a forensic search of a computer is conducted" in this case was unconstitutionally unreasonable, (Doc. 69 at 9), Defendant should have been able to point to some investigative step described in that report, or to some file or thing that the examiner isolated.

Even if Defendant were to have made a motion based on these types of facts about the forensic examination, Defendant would still need to present some sort of legal argument as to why those facts show the examination was improper. This would be difficult. Courts have held generally that a "computer search may be as extensive as reasonably required to locate the items described in the warrant," *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006), making the play-by-play conduct of the examiner generally irrelevant to a motion to suppress. Notably, Defendant's second motion cites not one case that required the suppression of electronic evidence because of the conduct of a forensic examiner.

Defendant cannot be excused from his burden because Defendant claims not to know "how [the examination] was done, what keywords or other search methods and forensic programs were used, the time, extent, and whether any attempts were made to restrict the search results to the particularized files." (Doc. 69 at 8). In fact, many of these things can be learned from discovery, as noted above. Regardless, arguments about who has better access to the facts are arguments about where the burden should lie, and the Sixth Circuit has unambiguously placed that burden with the Defendant. *See Giacalone*, 853 F.2d at 482 (rejecting defendant's

argument that placing the burden upon him was " 'Kafkaesque' because all the evidence relating to the government's compliance with the minimization requirement remained in the government's possession"). Not surprisingly, other circuits also uniformly assign the burden to the party seeking suppression. *See United States v. Vilches-Navarrete*, 523 F.3d 1, 15 (1st Cir. 2008); *United States v. Waldrop*, 404 F.3d 365, 368 (5th Cir. 2005); *United States v. Ramirez-Garcia*, 269 F.3d 945, 947 (9th Cir. 2001) (requiring "facts which are sufficiently definite, clear, and specific to enable the trial court to conclude that contested issues of fact exist"); *United States v. Torres*, 191 F.3d 799, 811 (7th Cir. 1999); *United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir.1980). A contrary rule would effectively allow a lengthy evidentiary hearing in every case; this would contend bitterly with "the need to prevent diversion of attention from the main issue of guilt or innocence" in criminal proceedings. *Franks*, 438 U.S. at 167.

Defendant's failure to provide any specifics yields another problem with holding a hearing: Any subpoena to an FBI forensic examiner on a broad subject such as "the execution of the warrant" would violate the Justice Department's *Touhy* regulations. Section 301 of Title 5 of the United States Code provides in part that the "head of an Executive department or military department may prescribe regulations for… the conduct of its employees… and the custody, use, and preservation of its records, papers, and property." 5 U.S.C. § 301. In *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951), the Supreme Court held that an FBI agent could not be held in contempt for refusing to produce certain documents subpoenaed by a state prisoner in a federal habeas proceeding where the FBI had not authorized disclosure under regulations issued pursuant to that statute. The Department of Justice's *Touhy* regulations are published at 28 C.F.R. §§ 16.21-29. Under 28 C.F.R. § 16.26(b), disclosure cannot be made if "[d]isclosure would reveal investigatory records compiled for law enforcement purposes, and would interfere

with enforcement proceedings or disclose investigative techniques and procedures the effectiveness of which would thereby be impaired." Obviously, asking FBI agents about how computer systems are searched and how forensic examinations are conducted would reveal investigative techniques. Similarly, the *Touhy* regulations require that when oral testimony is subpoenaed, "a statement by the party seeking the testimony or by the party's attorney setting forth a summary of the testimony sought must be furnished." 28 C.F.R. § 16.23(c). Given that Defendant is unable to provide this Court with any criticism of the forensic examiner's conduct beyond his use of a search technique that was described in advance in the warrant application, it is unlikely Defendant will be able to comply.

III. THERE ARE NO GROUNDS FOR SUPPRESSION OF ANY EVIDENCE

In addition to being remarkable for its failure to identify any fault with probable cause or any improperly seized file, Defendant's motion is notable for its scope: it does not ask for suppression of particular files, but of "*all* evidence obtained as a result of the… search of the computer" (Doc. 69 at 27).

Defendant asks for suppression of everything even while he agrees that the first warrant authorized the seizure of "some of his computer files." (Doc. 20 at 6). Defendant, then, is potentially asking for the suppression of things whose seizure he agrees was authorized by the warrant. Suppression is an extraordinary remedy in any case, used only as a "last resort," *Hudson v. Michigan,* 547 U.S. 586, 591 (2006), and only when its deterrent effect is "worth the price paid by the justice system," *Herring v. United States*, 129 S.Ct. 695, 702 (2009). Suppression of ***everything,*** even though some things were lawfully seized, is almost unheard of.

"Unlawful seizure of items outside a warrant does not alone render the whole search invalid and require suppression of all evidence seized, including that lawfully taken pursuant to

the warrant." *United States v. Lambert*, 771 F.2d 83, 93 (6th Cir. 1985). Even if Defendant were to prevail in his argument that too many items were seized, "where the extra-warrant items were not received into evidence against the defendant," there is no prejudice and the "search does not become invalid." *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988). "[I]nfirmity due to overbreadth does not doom the entire warrant; rather, it requires the suppression of evidence seized pursuant to that part of the warrant but does not require the suppression of anything described in the valid portions of the warrant." *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001) (internal quotation marks and ellipses omitted).

Defendant's second motion to suppress cites not a single case authorizing blanket suppression of all evidence from a computer search. This failure supports rejecting Defendant's second suppression motion. Reading Defendant's motion charitably, Defendant appears to be repeating (without citation) his earlier argument that agents acted in "flagrant disregard" of the warrant. (Doc. 20 at 10). Blanket suppression is appropriate only when "officers engaged in an impermissible general search," which occurs when "their search ***unreasonably*** exceeded the scope of the warrant." *United States v. Garcia*, 496 F.3d 495, 507 (6th Cir. 2007). Given that Defendant concedes the warrant authorized the seizure of "some of his computer files," (Doc. 20 at 6), and given that Defendant does not identify a single file that fell outside that set of properly seizeable files, Defendant has simply failed to make this argument.

Finally, as noted above, the affidavits in support of both warrants plainly stated that the entire computers would be seized and that all files would be examined. (*See supra* at I.A). Any argument that the officers "unreasonably exceeded the scope" of a warrant that was obtained after the officers informed the magistrate judge of possible search techniques is simply unsupportable. At the very least, this means that the "officer's reliance on [the] warrant is

objectively reasonable," *United States v. Higgins,* 557 F.3d 381, 390 (6th Cir. 2009), and therefore suppression would alternatively be improper under *United States v. Leon,* 468 U.S. 897 (1984). Of course, this alternative argument need not be addressed given the ample probable cause and express authority for the examination of the Acer laptop provided in the search warrants.

Respectfully submitted this 3rd day of August, 2009.

JAMES R. DEDRICK
United States Attorney

s/ D. Gregory Weddle
s/ Mark L. Krotoski
s/ Josh Goldfoot

D. Gregory Weddle
Assistant U.S. Attorney
800 Market Street, Suite 211
Knoxville, TN 37902
865-225-1710

Mark L. Krotoski
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Ave. NW
Washington, DC 20005

Josh Goldfoot
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Ave. NW
Washington, DC 20005

CERTIFICATE OF SERVICE

I hereby certify that on August 3, 2009, a copy of the foregoing Opposition to Defendant's Second Motion to Suppress and Motion for Evidentiary Hearing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. All other parties will be served by regular U.S. mail. Parties may access this filing through the Court's electronic filing system.

s/ D. Gregory Weddle
D. Gregory Weddle
Assistant U.S. Attorney
800 Market Street, Suite 211
Knoxville, TN 37902
865-225-1710